

EXHIBIT J

Melissa H. Nafash (N.Y. Bar No. 4816328)
Jonathan Gardner (N.Y. Bar No. 2384394)
Shannon K. Tully (N.Y. Bar No. 5732235)

LABATON SUCHAROW LLP

140 Broadway, 34th Fl.
New York, NY 10005
Telephone: (212) 907-0700
Facsimile: (212) 818-0477
mnafash@labaton.com
jgardner@labaton.com
stully@labaton.com
Attorneys for Claimant

BEFORE THE AMERICAN ARBITRATION ASSOCIATION

PAULA WALLRICH

Claimant,

v.

SAMSUNG ELECTRONICS AMERICA, INC.; and
SAMSUNG ELECTRONICS CO., LTD. (d/b/a
Samsung Electronics America, Inc.),

Respondents.

DEMAND FOR ARBITRATION

Claimant, **Paula Wallrich**, by counsel, brings this arbitration against to Samsung Electronics America, Inc. and Samsung Electronics Co., Ltd. (d/b/a Samsung Electronics America, Inc.) (collectively “Samsung” or “Respondents”) to redress and put a stop to Respondents’ surreptitious collection, use, storage, and disclosure of Claimant’s sensitive biometric data in violation of Illinois’ Biometric Information Privacy Act (“BIPA”).

PARTIES

1. **Paula Wallrich** (*hereinafter* “Claimant”) is a natural person who owns a Samsung Galaxy Device and has taken photographs of themselves, including photographs of Claimant’s face and other physical attributes while residing in the State of Illinois, and saved those photographs to the Samsung Gallery application.

2. Samsung Electronics America, Inc., the designer, manufacturer, and vendor of Samsung smartphones, tablets, and apps,¹ is a corporation organized under New York with its principal place of business in New Jersey. Samsung has nearly a 30% market share of the smartphone market in the United States, and a 17.6% market share of the tablet market. Since 2009, Samsung has sold over 2 billion “Samsung Galaxy” (formerly stylized as “Samsung GALAXY”) smartphone devices and more than 50 million “Galaxy Tab” devices (collectively “Samsung Devices”) within the last two years. The Samsung Galaxy product line includes the popular Galaxy S, Galaxy Note, Galaxy Z, Galaxy A (Alpha), and Galaxy M (Millennial) series. Samsung is the designer, manufacturer, and vendor of Samsung smartphones, tablets, and apps. Samsung Electronics America, Inc. is a wholly-owned subsidiary of Samsung Electronics Co., Ltd.

3. Samsung Electronics Co., Ltd. (f/k/a Samsung Electronic Industries), a South Korean multinational electronics corporation headquartered in the Yeongtong District of Suwon, was incorporated under the laws of the Republic of Korea in 1969 and lists its shares on the Korea Stock Exchange in 1975. Samsung Electronics Co., Ltd. is the parent company to Samsung Electronics America, Inc.

JURISDICTION AND VENUE

4. Respondents’ Terms of Use agreement contains a mandatory arbitration provision wherein the user and Respondents agree to the following:

- a) Any dispute, claim or controversy arising out of or relating in any way between Claimant and Respondents shall be determined by binding arbitration.

¹ Samsung has nearly a 30% market share of the smartphone market in the United States, and a 17.6% market share of the tablet market. Tablet Vendor Market Share United States of America (June 2021), available <https://gs.statcounter.com/vendor-market-share/tablet/united-states-of-america>. Mobile Fact Sheet, Pew Research Center (Apr. 7, 2021), available at <https://www.pewresearch.org/internet/fact-sheet/mobile/>.

- b) The arbitration shall be conducted on an individual basis and not as a class.
- c) The arbitration shall be conducted before the American Arbitration Association (“AAA”).
- d) Administrative, facility, and arbitrator fees for arbitrations in which the total damages exceed \$5,000.000 are determined according to the AAA rules.
- e) Claimant can opt-out of the arbitration provision within 30-days of the date Claimant agrees to the Terms.
- f) The laws of the State of New York, to the extent not preempted by or inconsistent with federal law, will apply.

5. Claimant elects to have the arbitration conducted solely based on the documents submitted to the arbitrator.

FACTUAL BACKGROUND

I. BIOMETRICS AND CONSUMER PRIVACY

6. “Biometrics” refers to measurable characteristics or processes used for identification. As a characteristic, biometrics is defined as “a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition.”² As a process, biometrics is defined as “automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics.”³

² <http://www.biometrics.gov/Documents/Glossary.pdf>. The term “biometrics” was developed and defined by the National Science & Technology Council's (NSTC) Subcommittee on Biometrics (2006), as updated.

³ <http://www.biometrics.gov/Documents/Glossary.pdf>.

7. Biometrics are used to identify individuals based on unique, distinctive, and measurable characteristics or features known as “biometric identifiers.”^{4,5}

8. “Biometric identifiers” are categorized by physiological and behavioral characteristics. Examples include, but are not limited to, face or hand geometry, fingerprints, palm prints, irises, retinas, veins, and DNA sequences. Behavioral based biometric identifiers “are apparent in a person’s interaction with the environment, such as signatures, gaits, and keystroke,”⁶ while “[v]oice/speech contains both behavioral features, such as accent, and physiological features, such as voice pitch.”⁷

9. Biometric technologies vary widely depending on the biometric identifier. Modern era biometric processes include:

- a. Face recognition,
- b. Fingerprint recognition,
- c. Hand geometry,
- d. Retina scan,
- e. Iris scan,
- f. Voice recognition,

⁴ “Biometrics: A general term used alternatively to describe a characteristic or a process: As a characteristic: A measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition. As a process: Automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics.” *Biometrics Foundation Documents*, NISTC Subcommittee on Biometrics (2009), <http://www.dtic.mil/dtic/tr/fulltext/u2/a505048.pdf>; Sushma Jaiswal, *et al.*, *BIOMETRIC: CASE STUDY*, J. GLOBAL RESEARCH IN COMPUTER SCIENCE (Oct. 2011), <https://www.rroij.com/open-access/biometric-case-study-19-49.pdf> (“A biometric is any measurable, robust, distinctive, physical characteristic or personal trait of an individual that can be used to identify, or verify the claimed identity of, that individual. Measurable means that the characteristic or trait can be easily presented to a sensor and converted into a quantifiable, digital format. This allows for the automated matching process to occur in a matter of seconds.”); Stephen Mayhew, *History of Biometrics* (Feb. 1, 2018), <https://www.biometricupdate.com/201802/history-of-biometrics-2>; *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1094 (N.D. Ill. 2017) (“Biometrics” refers to “biology-based set[s] of measurements”).

⁵ Sushma Jaiswal, *et al.*, *BIOMETRIC: CASE STUDY*, J. GLOBAL RESEARCH IN COMPUTER SCIENCE (Oct. 2011), <https://www.rroij.com/open-access/biometric-case-study-19-49.pdf>

⁶ *Id.*

⁷ *Id.*

- g. Vascular or vein recognition,
- h. Skin texture,
- i. DNA,⁸
- j. Dynamic signature verification,⁹
- k. Keystroke dynamics, and
- l. Gait analysis.

10. One of the most prevalent uses of biometrics is in facial recognition technology, which records the “spatial geometry” or more commonly known as “facial geometry” of distinguishing features of the face.¹⁰ These distinguishing features include the nose, eyes, eyebrows, mouth, chin, and lips.¹¹ The graphic in Figure 1 below illustrates the way “face geometry” is commonly used to refer to the location and spatial relationships between the distinguishing features.



Figure 1¹²

⁸ The National Biometrics Challenge, National Science and Technology Council Subcommittee on Biometrics and Identity Management, (September 2011) at p. 14, available at:

<https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/biometricchallenge2011.pdf>

⁹ Dynamic Signature, available at <http://www.biometrics.gov/Documents/DynamicSig.pdf>

¹⁰ <https://www.biometric-solutions.com/face-recognition.html>

¹¹ Sushma Jaiswal, et al., *BIOMETRIC: CASE STUDY*, J. GLOBAL RESEARCH IN COMPUTER SCIENCE (Oct. 2011),

<https://www.rroij.com/open-access/biometric-case-study-19-49.pdf>

¹² Daniel Thomas, *Future airports could become hi-tech pleasure dome* BBC NEWS (Feb. 2, 2015), <https://www.bbc.com/news/business-30830296>

11. Facial recognition technology works by: (1) scanning¹³ a photograph and/or digital image to detect a human face, (2) extracting the distinguishing facial features, such as the nose, eyes, mouth, chin, ear, and their relative portions in the digital image that are based on specific details about the face geometry as determined by facial points and contours and their relative portions in the digital image, (3) generating a face “template,” (or “faceprint”), and (4) comparing the resulting “face template” to the face templates stored in a “faceprint database” for identification.¹⁴

12. The recent sophistication of facial recognition software has generated many commercial applications of the technology but has also raised serious privacy concerns about its massive scale, scope, and surreptitiousness.¹⁵

13. The use of biometric data presents unique risks. Biometric data is one of the most sensitive forms of personal information because—unlike other types of data such as account or ID numbers—biometric data cannot be changed if stolen or compromised. Once a person’s unique and permanent biometric identifiers are exposed, she has no way to prevent identity theft and unauthorized tracking.

14. Proprietary biometric data collected by companies—especially those who collect it unlawfully and without permission—can be leaked, hacked, exposed, or otherwise exploited, as

¹³ A software program can be said to “scan” a digital image to detect a face by identifying key facial landmarks or features such as the nose, mouth, eyes and chin. See Belhumeur, *Localizing Parts of Faces Using a Consensus of Exemplars*, 2011 IEEE Conference on Computer Vision and Pattern Recognition (CPVR) (2011) (“Many fiducial point detectors include classifiers that are trained to respond to a specific fiducial (e.g., left corner of the left eye). These classifiers take as input raw pixel intensities over a window or the output of a bank of filters (e.g., wavelets, Gaussian Derivative filters, Gabor filters, or Haarlike features). These local detectors are scanned over a portion of the image and may return one or more candidate locations for the part or a “score” at each location.”).

¹⁴ <https://www.biometric-solutions.com/face-recognition.html>

¹⁵ *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy Tech & the Law of the S. Comm. on the Judiciary*, 112th Cong. 1 (2012) (statement of Jennifer Lynch, Staff Attorney, Electronic Frontier Foundation), available at https://www.eff.org/files/filenode/jenniferlynch_eff-senate-testimony-face_recognition.pdf.

demonstrated by the highly publicized breach of the Clearview AI scandal and the Respondent and Cambridge Analytica scandal.

15. Recognizing that the private sector continuously violates a person's right to privacy of their biometric data, on August 4, 2020, Senators Merkley and Sanders introduced the National Biometric Information Privacy Act of 2020 ("NBIPA"), which is groundbreaking legislation that would prohibit *private* companies from collecting biometric data.¹⁶

16. Unlike other identifiers such as Social Security or credit card numbers, which can be changed if compromised or stolen, biometric identifiers linked to a specific voice or face cannot. These unique and permanent biometric identifiers, once exposed, leave victims with no means to prevent identity theft and unauthorized tracking.

17. Due to the clear potential for invasion of privacy by companies who gather biometric data, the Federal Trade Commission ("FTC") urged companies using facial recognition technology and collecting biometric data to ask for clear consent before scanning and extracting biometric data from their digital photographs.¹⁷

18. Efforts to regulate the use of facial recognition and biometric data have continued. In the Summer of 2015, the National Telecommunications and Information Administration ("NTIA") held a workshop in an attempt to create a code of conduct for the use and operation of facial recognition technology. Present at the meeting were trade associations representing some of the largest technology companies in the world, including companies like Google and Microsoft,

¹⁶ See Merkley, *Sanders Introduce Legislation to Put Strict Limits on Corporate Use of Facial Recognition*, <https://www.merkley.senate.gov/news/press-releases/merkley-sanders-introduce-legislation-to-put-strict-limits-on-corporate-use-of-facial-recognition-2020>. The Bill can be accessed at: <https://www.merkley.senate.gov/imo/media/doc/20.08.04%20National%20Biometric%20Information%20Privacy%20Act.pdf>.

¹⁷ See *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, Federal Trade Commission (Oct. 2012), available at <http://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognitiontechnologies/121022facialtechrpt.pdf>.

advocates, experts, and members of the public interest community. But these talks quickly fell through—ending with the entire public interest community staging a walk out before the meeting had ended—because not a single technology trade association “would agree that before you use facial recognition to identify someone by name, even if you don’t have any relationship with that person, you need to get their consent.”¹⁸

19. Companies have only continued to exploit facial recognition technology and the use of biometric data. For example, for eight years, RiteAid deployed facial recognition systems in largely lower-income, non-white neighborhoods, allegedly to target these demographics specifically.¹⁹ Such continued abuses of facial recognition technology and biometric data that harm the public welfare led to the enactment of the Illinois Biometric Information Privacy Act.

A. Facial Recognition Technology and Facial Processing Systems

20. Facial recognition technology is one form of technology that processes faces.

21. There are three main categories of facial processing technology: (1) facial detection; (2) facial analysis; and (3) facial recognition or identification.

22. Facial detection determines whether the image contains a face, and can also be used to determine whether any face is present and where the face is location.

23. Facial analysis technology enables the detection of various facial characteristics, also known as landmark features. Facial analysis enables facial recognition by comparing an individual’s facial features to available images for verification or identification purposes.²⁰

¹⁸ *Biometrics Are Coming, Along With Serious Security Concerns*, WIRED (Mar. 9, 2016), <https://www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/> (last visited Sept. 29, 2021).

¹⁹ <https://www.reuters.com/investigates/special-report/usa-riteaid-software/>

²⁰ Testimony provided on Feb. 6, 2020, by Dr. Charles H. Romine, Director, Information Technology Laboratory, NIST, United States Department of Commerce, to the Committee on Homeland Security, U.S. House of Representatives. <https://www.nist.gov/speech-testimony/facial-recognition-technology-frt->

24. Facial recognition technology (“FRT”) confirms a photo matches a different photo of the same person in a facial template database.

25. FRT is based on algorithms that learn how to recognize human faces and the hundreds of ways in which each one is unique.

26. These algorithms create a unique “face template” of a person’s facial geometry by scanning, identifying, and measuring various facial landmarks, such as the location of the mouth, chin, nose, ears, eyes, and eyebrows.

27. To automatically extract face templates from new images, a facial recognition algorithm must be “trained” to identify and measure the relevant facial landmarks.

28. This is typically accomplished by the algorithm evaluating “triplet” sets of photographs—i.e., two images of the same person (known as the “anchor” and “positive sample”), and one of a completely different persons (known as the “negative sample”).

29. The algorithm reviews the measurements collected from each image, and then adjusts itself so that the measurements collected from the anchor sample are closer to those collected from the positive sample, and further apart from those collected from the negative sample.

30. After repeating this process a few times, the algorithm learns to reliably scan for and collect a face template of the geometry of any given face.

B. Deep-learning Facial Recognition and Processing Techniques

31. Biometric recognition methods utilize deep learning-based models to provide an end-to-end learning framework, which can jointly learn the feature representation while performing classification. This is achieved through a multi-layer neural network, also known as Deep Neural Networks (“DNN”), to learn multiple levels of representations that correspond to different levels of abstraction, which is better suited to uncover underlying patterns of the data.

32. Facial recognition is a biometric technology that identifies facial vectors and features and matches them to a individual pre-enrolled in a database. In the mid-2000s, the technology based on digital signal processing techniques (“DSP”) was restricted to frontal-facing images. However, more recently, there has been a dramatic improvement in precision advancements of artificial technologies (“AI”) based DNNs leading to the development of AI-based facial recognition engine. AI based FRT leverages proprietary AI algorithms and mathematical equations to make its connections to individuals by measuring a number of facial variables, such as nose depth and width, forehead length, and eye shape, and saves the information as a template. The template generated for an individual is used as a basis for comparison to confirm identity if there is a match with an existing template.

33. The key features of a facial recognition engine are face detection, face feature extraction, and face recognition. Face detection is the first step the technology takes to detect a face. Face detection works by scanning the entire image, video, and/or scene to determine if the frame contains full or partial human faces. Once a face is detected, the engine extracts a n-dimensional vector set creating a face template from the face image. The face template that is extracted from the individual’s face is used for matching or searching. The newly extracted face template is then matched to pre-existing templates in a database. A 1:N search is performed by matching an individual’s template to the entire database to find the best match and confirm identity.

II. ILLINOIS’S BIOMETRIC INFORMATION PRIVACY ACT

34. The Illinois Legislature has found that “[b]iometrics are unlike other unique identifiers” such as social security numbers, which can be changed if compromised. 740 ILCS 14/5(c). “Biometrics . . . are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.” *Id.*

35. In 2008, to protect Illinois residents from the surreptitious collection and use of their biometric data, the Illinois Legislature enacted BIPA.²¹ Under BIPA:

(b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:

(1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;

(2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

(3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

...

(d) No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:

(1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure[.]

740 ILCS 14/15(b) and (d).

36. BIPA applies to entities that interact with two forms of biometric data: "biometric identifiers"²² and "biometric information." 740 ILCS 14/15(a)-(e).

²¹ In passing BIPA, the Illinois Legislature found that (1) "[b]iometrics are unlike other unique identifiers . . . [and] are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions" (740 ILCS 14/5(c)); (2) "[a]n overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information" (740 ILCS 14/5(d)); (3) "[t]he full ramifications of biometric technology are not fully known" (740 ILCS 14/5(f)); and (4) "[t]he public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information" ((740 ILCS 14/5(g)).

²² "Biometric identifiers" are categorized by physiological and behavioral characteristics. Examples include, but are not limited to, voiceprints, face or hand geometry, fingerprints, palm prints, iris patterns, retina patterns, veins, and DNA sequences.

37. “Biometric identifiers” means “a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.” 740 ILCS 14/10.²³ However, BIPA only provides a non-exhaustive list of biometric identifiers, and the legislative intent behind BIPA was to protect its residents from irreputable harm by placing strict requirements on companies regarding the collection, usage, storage, retention, and destruction of unique and highly sensitive biometric identifiers and information.

38. “A person cannot obtain new DNA or new fingerprints or new eyeballs for iris recognition, at least not easily or not at this time. Replacing a biometric identifier is not like replacing a lost key or a misplaced identification card or a stolen accesscode. The Act’s goal is to prevent irretrievable harm from happening and to put in place a process and rules to reassure an otherwise skittish public.” *Sekura v. KrishnaSchaumburg Tan, Inc.*, 2018 IL App (1st) 180175, ¶ 59, 115 N.E.3d 1080, 1093, *appeal denied*, 119 N.E.3d 1034 (Ill. 2019).

39. “Biometric information” consists of biometric identifiers used to identify an individual. BIPA defines “biometric information” to include “any information, regardless of how it is captured, converted, stored, or shared, based on an individual’s biometric identifier used to identify an individual.” *Id.*; *Rivera v. Google Inc.*, 238 F.Supp.3d 1088, 1090 (2017) (“The Act also bans the non-consensual collection and storage of *information...that is ‘based on’ those biometric identifiers.*”) (emphasis added).²⁴

²³ See also, *Sekura v. KrishnaSchaumburg Tan, Inc.*, 2018 IL App (1st) 180175, ¶ 59, 115 N.E.3d 1080, 1093, *appeal denied*, 119 N.E.3d 1034 (Ill. 2019) (“A person cannot obtain new DNA or new fingerprints or new eyeballs for iris recognition, at least not easily or not at this time. Replacing a biometric identifier is not like replacing a lost key or a misplaced identification card or a stolen accesscode. The Act’s goal is to prevent irretrievable harm from happening and to put in place a process and rules to reassure an otherwise skittish public.”).

²⁴ See also *In re Clearview Privacy Litigation*, No. 21-cv-00135, at p. 8 (N.D. Ill. Feb. 14, 2022) (Coleman, S.) *citing* *Flores v. Motorola Solutions, Inc.*, No. 21-cv-1128, 2021 WL 232627, at *3 (N.D. Ill. Jan. 8, 2021) (Norgle, J.) (“The Court cannot say that those protections do not apply to any publicly published photographs of individuals—especially given that the biometric data in this case is the facial geometry of the class members, in contrast to the photos themselves.”); *Rivera*, 238 F.Supp.3d at 1096 (“‘biometric identifier’ is not the underlying medium itself, or a way of

40. BIPA imposes various requirements on private entities that collect or maintain biometric data and requires a company to develop a publicly available written policy establishing a retention schedule and guidelines for permanently destroying biometric data when the initial purpose for collecting such data has been satisfied or within three years of the individual's last interaction with the company, whichever occurs first. 740 ILCS 14/15(a).

41. Under BIPA, "[a] prevailing party may recover *for each violation*: (1) against a private entity that negligently violates a provision of this Act, liquidated damages of \$1,000 or actual damages, whichever is greater; (2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of \$5,000 or actual damages, whichever is greater; (3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and (4) other relief, including an injunction, as the State or federal court may deem appropriate." *Id.* (emphasis added).

42. Each part of section 15 described above "imposes various duties upon which an aggrieved person may bring an action under section 20... as section 20 provides that a 'prevailing party may recover for each violation' (740 ILCS 14/20), a plaintiff who alleges and eventually proves violation of multiple duties could collect multiple recoveries of liquidated damages. *Id.* § 20(1), (2)." *Tims v. Black Horse Carriers, Inc.*, 2021 IL App (1st) 200563, ¶ 30, 2021 WL 4243310, at *5 (Ill.App. 1 Dist., 2021).

III. RESPONDENTS GENERATES, COLLECTS, STORES, RETAINS, SHARES, AND PROFITS FROM THE BIOMETRIC IDENTIFIERS OF SAMSUNG USERS IN VIOLATION OF ILLINOIS LAW

43. Illinois enacted BIPA as an informed consent statute, specifically imposing safeguards to ensure that individuals' privacy rights and control over their biometric identifiers

taking measurements, but instead is a set of measurements of a specified physical component (eye, finger, voice, hand, face) used to identify a person.").

and biometric information are properly honored and protected and impose liability on private entities who fail to comply with the statutory requirements. 740 ILCS § 14/1, *et seq.*²⁵

44. BIPA defines “biometric identifier” to mean a “retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.” 740 ILCS § 14/5. Moreover, biometric information is defined as “any information, *regardless* of how it is captured, converted, stored, or shared, based on an individual’s biometric identifier used to identify an individual.” 740 Ill. Comp. Stat. Ann. 14/10 (emphasis added).

45. The Samsung Devices are manufactured and sold with the Gallery App pre-installed as the default photo and video application. In direct violation of BIPA, Samsung collects, uses, and stores the biometric identifiers, including face scans and faceprints, and biometric information such as facial geometry of Illinois residents without valid consent and without complying with BIPA’s requirements. Samsung’s BIPA violations are evidenced by: (1) the functionality of the Gallery App, (2) application and use of facial processing systems, algorithms, and facial recognition techniques; and (3) use and continued development of systems and methods that collect facial data as evidenced by numerous patents issued by the United States Patent Office (“USPTO”) to Samsung discussing the use of and/or application of facial and/or face recognition technology, techniques for scanning facial geometry, and collection and use of facial geometry and related data.²⁶

²⁵ BIPA governs the retention, collection, disclosure, and destruction of retained biometric identifiers or biometric information, and prohibits a private company from capturing, purchasing, receiving through trade, or otherwise obtaining biometrics without first informing the subject and obtaining written consent. *See* 740 ILCS 14/15(a)-(e).

²⁶ *See, e.g.,* See Patent No. US 10,666,869 B2: Image Display Apparatus and Image Display Method (May 26, 2020), (“Referring to FIG. 2 again, in operation S130, the subject included in the captured image may be recognized through face recognition. Whenever the image is captured, the control unit 150 may perform the face recognition on the captured image. The control unit 150 may recognize the subject included in the captured image by comparing a face of the subject included in the captured image with a database. For example, the control unit 150 may recognize the subject included in the captured image within persons included in a contact list. The control unit 150 may separately perform the face recognition on each captured image...In operation S140, at least one of a tag

A. Gallery App

46. The Samsung Devices are manufactured and sold with the Gallery App pre-installed as the default photo and video viewing application.

47. Using the Gallery App, Samsung users can create personal and shared albums, “stories,”²⁷ and movies, and employ Samsung’s editing and “tagging” features.²⁸

48. According to Samsung, the Gallery App allows Samsung Device users to save, organize, edit, share, and store their photos in one location:

The Gallery app is the perfect place to organize all of your videos and photos. Everything you capture from the camera on your phone will automatically be saved to the gallery, but you can also add in or download photos so that you can store all of your memories in the same place. If you want greater control over how your images and videos look, the Gallery has a full suite of editing options from filters and stickers to colour tools and background music.

The Gallery app can connect to the Samsung Cloud, making it really easy to share your unforgettable moments across all of your devices. You can also create shared albums so that all of your loved ones can follow along with your adventures, no matter where you are in the world.²⁹

corresponding to the recognized subject and a share button may be displayed on the camera preview screen. *The display unit 120 may display the tag corresponding to the subject recognized from the captured image* on the camera preview screen. The tag corresponding to the recognized subject may include a name, a nickname, or a photo of the recognized subject.”) (emphasis added).

²⁷ *How do I use the Gallery app on my Galaxy device?* SAMSUNG, <https://www.samsung.com/uk/support/mobile-devices/how-do-i-use-the-gallery-app/> (last viewed Mar. 10, 2022) (“Stories give you everything you need to enhance your images and create something even more shareable. You can use stories in a similar way to albums, helping you to organize your image and videos but you can also use stories to turn your images into collages and GIFs.”); *see also*, *id.* at “Gallery Settings” (allowing users to “create stories automatically based on the faces, time, and locations of pictures and videos”)

²⁸ *Id.* (According to Samsung, its editing tools include “a huge range of options including filters, stickers, doodles and colour spot”).

²⁹ *How do I use the Gallery app on my Galaxy device?* SAMSUNG, <https://www.samsung.com/uk/support/mobile-devices/how-do-i-use-the-gallery-app/> (last viewed Mar. 10, 2022).

49. Once a photo or video is captured, Samsung automatically scans and analyzes the image and/or video frame, assigns a tag³⁰ based on the object(s), face, and/or individual(s) identified, and saves it to the user's default Gallery App.

50. Once a face is detected, Samsung's algorithm identifies and extracts key landmark facial features, such as the location of the mouth, chin, nose, ears, eyes, and eyebrows, to calculate a unique digital representation of each face.

51. Using this information, Samsung creates a face template based on the identified geometric attributes such as distance between the eyes and the width of the nose. The newly created face template is compared to the face templates stored in Samsung's database to identify a match, which may include individuals within the person's contact list.³¹

52. The Gallery App uses the face templates that are extracted from the individual's face to match, search, organize, sort, and group images of the same user into one location. This is accomplished by comparing the pre-existing face templates stored in Samsung's database to the newly extracted face template. These face templates each constitute a "biometric identifier." *See* 740 ILCS 14/10.

53. If there is a match, the Gallery App tags the image and groups it with previously stored images depicting the same individual. Images of the same individual are "stacked" together like a deck of cards. The front of the stack displays the identified individual's face within a circular frame.

³⁰ *Id.* ("The Gallery app will automatically assign tags to many of your photos by analysing what is in the image. This can help you sort through your photos, create an album of similar images or search for a specific photo."); <https://r2.community.samsung.com/t5/Galaxy-S/camera-image-processing/td-p/4109995>.

³¹ Patent No. US 10,666,869 B2: Image Display Apparatus and Image Display Method (May 26, 2020) ("The image display method may further include recognizing subjects included in the captured one or more images through face recognition, displaying tags corresponding to the recognized subjects and a share button on the camera preview screen, and sharing the captured one or more images in response to a touch input on the photo reel, at least one of the thumbnails, at least one of the tags, or the share button."); Patent No. US 10,129,481 B2: Image Display Apparatus and Image Display Method (Nov. 13, 2018) (same).

54. Samsung stores the face templates extracted from the user's photo library, at minimum, in a facial recognition database, or facial database, in the solid state memory on the user's Samsung Device. The Gallery App uses these face templates to organize and sort photos based upon the particular individuals who appear in the photos. This is accomplished by comparing the face templates of individuals who appear in newly stored photos against those already saved in the facial database. If there is a match, the Gallery App groups the newly uploaded photo with previously stored photos depicting the same individual.

55. Tagging" is accomplished through Samsung's proprietary facial processing systems and recognition technology, otherwise known as Samsung's face recognition feature, which uses an algorithm to scan images captured to detect a face.

56. The Gallery App also employs other face scanning processes and techniques such as image analysis. Specifically, the Gallery App uses image analysis to "classify images based on what's in them, such as people, backgrounds, and objects, so you can search for them more easily" and "create stories automatically based on the faces, times, and locations of pictures and videos."³² In other words, Samsung's proprietary software and algorithms repeatedly scan and analyze photos and videos to understand and distinguish what objects, scenes, humans, animals, and landscapes are present. More importantly, the system uses the facial geometry of the individual to identify and recognize their face, automatically apply a tag, and stack the related images of that specific individual.

57. As the Gallery App applies facial scanning and face recognition techniques automatically to all photos and videos, Samsung Device users cannot disable the feature nor consent to its uses. Moreover, neither Samsung's privacy policy nor the Gallery App contain any

³² *How do I use the Gallery app on my Galaxy device?* SAMSUNG, <https://www.samsung.com/uk/support/mobile-devices/how-do-i-use-the-gallery-app/> (last viewed Mar. 10, 2022) at "Can I sync my photos across my devices?"

type of disclosure to notify Illinois users that Samsung is generating, collecting, using, and storing their biometric information and biometric identifiers. The Gallery App also purposefully misleads users into thinking that Samsung applies non-facial recognition processes by disclosing its use of “image analysis” while failing to notify users that this system cannot function without repeatedly scanning their facial geometry and generating face scans.

58. Moreover, through its Gallery App, Samsung creates a unique face template for every face detected in the photographs stored on the user’s Samsung Device. This is an automated process that occurs without the user’s involvement or consent whenever a new photograph is stored on a Samsung Device users cannot disable this facial recognition technology, nor can they prevent Samsung from harvesting the biometric identifiers (*i.e.* scans of face geometry) from the photographs stored on their Samsung Devices.

59. Samsung provides no mechanism by which anyone may opt out of this process. Consumers who buy Samsung Devices own the hardware, but merely license the software necessary for the device to function. That software is wholly owned and controlled by Samsung, as confirmed by Samsung’s End User License Agreements (“EULAs”). The EULAs provide, in pertinent part:

Samsung grants you a limited non-exclusive license to install, use, access, display and run one copy of the Samsung Software on a single Samsung Mobile Device[.] *** Samsung reserves all rights not expressly granted to you in this EULA. The Software is protected by copyright and other intellectual property laws and treaties. Samsung or its suppliers own the title, copyright and other intellectual property rights in the Samsung Software. The Samsung Software is licensed, not sold.³³

60. Under the terms of the EULAs, the Samsung Device user is prohibited from modifying or altering the software.

³³ <https://www.samsung.com/sg/Legal/SamsungLegal-EULA/>

61. Because disabling facial recognition is not permitted by Samsung, the use of Samsung Devices to take or store photographs is *conditioned* on the collection of biometrics.

62. Samsung indiscriminately collects Biometrics for all photographic subjects, including customers, non-customers, and minors incapable of providing informed consent.

63. Samsung's Privacy Policy, in a supplement for California residents, confirms that "biometric information" is among the types of personal information Samsung collects.³⁴

64. Although, on information and belief, Samsung does not store or transfer all user biometrics on or by means of its servers, it has complete and exclusive control over the biometrics collected and stored on Samsung Devices. To be clear, Samsung controls:

- a. Whether biometric identifiers are collected;
- b. What biometric identifiers are collected;
- c. The type of biometrics that are collected and the format in which they are stored;
- d. The facial recognition algorithm that is used to collect biometrics;
- e. What biometrics are saved;
- f. Whether information based on biometric identifiers is used to identify users (thus creating biometric information);
- g. Whether biometrics are kept locally on users' Samsung Devices;
- h. Whether biometrics are encrypted or otherwise protected; and
- i. How long biometrics are stored.

Illinois courts have already ruled that storage of an individual's biometric data is a direct violation of Section 15(a) of BIPA regardless of whether the biometric information is stored on

³⁴ See Samsung Privacy Policy for the U.S., available at <https://www.samsung.com/us/account/privacy-policy/>.

the individual's device or the company's server. *See Hazlitt v. Apple Inc.*, 543 F.Supp.3d 643, 649-50 (S.D.Ill., 2021). For example, in *Hazlitt v. Apple Inc.*, Apple argued that plaintiffs lacked standing to pursue a BIPA claim under Sections 15(a)-(c) because Apple never stored plaintiffs' biometric information; instead, plaintiffs' biometric data was stored locally on each individual's smartphone device rather than a shared server. The Southern District of Illinois rejected Apple's argument explaining that storage of the data on plaintiffs' devices did not absolve the risk of harvesting the biometric data at a future time or prevent exposure of the information if breached:

Nevertheless, the Court disagrees that Plaintiffs' continued interaction with Apple deprives them of Article III standing. Plaintiffs allege that the durability of solid-state memory in Apple Devices creates a nearly permanent risk of a data breach of biometric identifiers and information, as the memory can last well past the natural life of the device user and, perhaps, *in perpetuity*. (*Id.* at ¶ 136). Plaintiffs also claim the biometric data may even persist on discarded Apple Devices, creating the risk of illicit harvesting of the data far into the future. (*Id.* at ¶ 138). The Court finds that this alleged unlawful retention of Plaintiffs' biometric information, potentially indefinitely, constitutes a privacy injury such that Plaintiffs have Article III standing to bring their BIPA section 15(a) claims.

Id.

65. The user of a Samsung Device, in contrast, has no ability to control the biometrics on the user's Samsung Device. The user has no control over whether biometrics are collected from the user's photo library. Users cannot disable the collection of biometrics or limit what information is collected or from whom it is collected. Indeed, Samsung's EULAs specifically *prohibit* users from modifying Samsung's software to prevent the collection of biometrics.³⁵ Thus, Samsung fully controls—and thus possesses—the biometrics on Samsung Device.

³⁵ <https://www.samsung.com/sg/Legal/SamsungLegal-EULA/> ("You shall not, and shall not enable or permit others to, copy, reverse engineer, decompile, disassemble, or otherwise attempt to discover the source code or algorithms of, the Software (except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation), or modify, or disable any features of, the Software, or create derivative works based on the Software. You may not rent, lease, lend, sublicense or provide commercial hosting services with the Software.").

B. Samsung's Camera Features Utilize Facial Processing and Recognition Techniques and Technology

66. Samsung boasts about its “legacy of innovative smartphone camera technology that makes it simpler for more people to take the perfect snapshot.”³⁶

67. The smartphone camera technology included within all Samsung Devices contains Samsung’s artificial intelligence (“AI”) operated “selfie camera” that employs facial processing techniques by repeatedly scanning the image frame to detect a user’s face.

68. Once the face is detected, Samsung’s algorithms use both the image and depth scanner to capture the individual’s facial landmark features, such as the mouth, chin, nose, ears, eyes, and eyebrows, and the spacing between those features.

69. Samsung then uses the facial landmarks to naturally enhance the faces of the detected individuals.

70. Most importantly, Samsung’s methodology falls squarely within the meaning of the term “face geometry.”³⁷

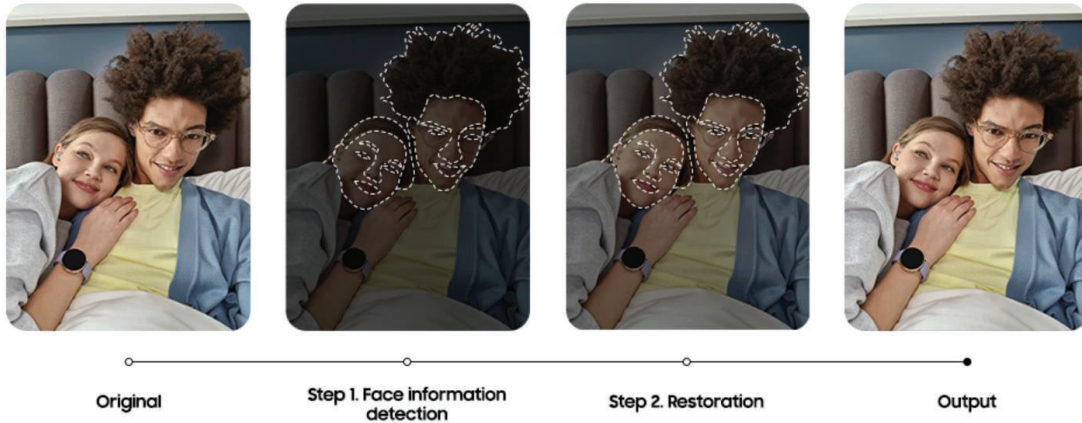
71. Samsung’s selfie camera technology is described and depicted in Figure 2 below.

³⁶ <https://news.samsung.com/global/behind-the-snapshot-how-the-galaxy-s21s-ai-improves-your-photos-in-the-blink-of-an-eye>

³⁷ See Peter N. Belhumeur, et al., *Localizing Parts of Faces Using a Consensus of Exemplars*, 2011 IEEE Conference on Computer Vision and Pattern Recognition (CPVR) (2011) (“Although faces come in different shapes, present themselves to the camera in many ways, and may possess often extreme facial expressions, there are strong anatomical and *geometric* constraints that govern the layout of face parts and their location in images.”).

Enhanced Selfie Experience

We've all had that moment of panic, frantically thumbing for the delete button, after taking a less than adequate selfie. But with the Galaxy S21 series' selfie camera, you'll always look your best with AI that delivers a more natural look and improved details. There are two key parts to the enhanced selfie experience:



1. Face information detection: When you snap a photo, the AI-powered selfie camera first identifies faces in the image, then segments them from the rest of the details in the scene, and finally applies natural enhancements to your subjects—all in the blink of an eye.

2. Restoration: The natural enhancements include bringing out the details in your subjects' hair, eyes, and facial features and adjusting white balance to create more natural looking skin tones in any environment. The results are instantly shareable photos that don't look overly processed or require further editing.

Samsung also included support for third party apps, so you can take images from your favorite camera or social media app and still get the benefits of AI-powered selfie camera.

Fig. 2³⁸

72. Similarly, Samsung's AI-powered cameras include object recognition and image processing and recognition technology, meaning that Samsung's camera repeatedly scans image and video frames to detect faces and objects. The repeated scanning and detection of faces is the first step of Samsung's facial recognition algorithm and used to later identify users by name and face templates.

³⁸ <https://news.samsung.com/global/behind-the-snapshot-how-the-galaxy-s21s-ai-improves-your-photos-in-the-blink-of-an-eye>; <https://www.nextpit.com/samsung-galaxy-s21-camera-ai>

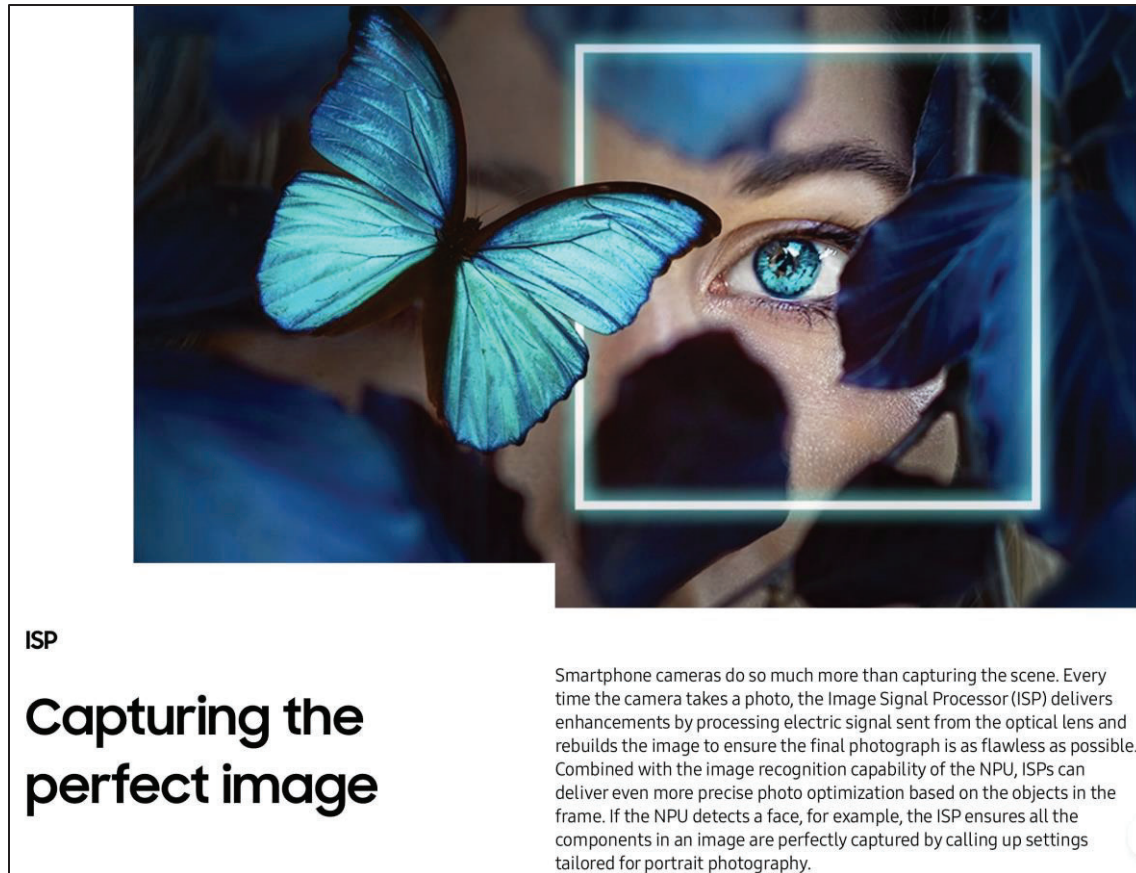


Fig. 3³⁹

C. **Samsung's Issued Patents Unequivocally Establish Its Biometric Data Collection and Storage Practices Violate BIPA**

73. Samsung's collection, use, and retention of biometric data is irrefutable.

74. For years, Samsung and its subsidiaries have researched, developed, and implemented various proprietary face detection, face-scanning, and facial recognition techniques, and mechanisms used to generate, capture, collect, share, and retain Claimant's sensitive biometric data without knowledge or consent.

75. Samsung presently uses and continues to develop systems and methods that scan, detect, identify, extract, use, collect, and store facial geometry; unique facial features or landmarks; and other methods and techniques to generate or create face scans and face signatures, as evidenced

³⁹ <https://semiconductor.samsung.com/insights/topic/ai/ai-camera/https://news.samsung.com/global/behind-the-snapshot-how-the-galaxy-s21s-ai-improves-your-photos-in-the-blink-of-an-eye>

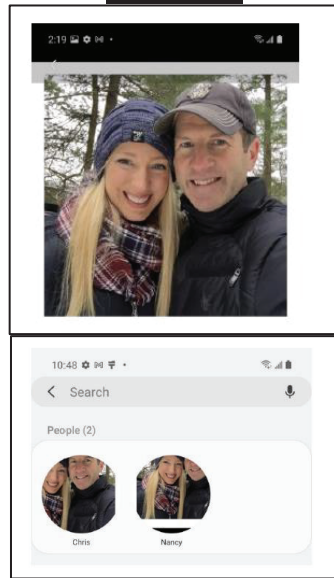
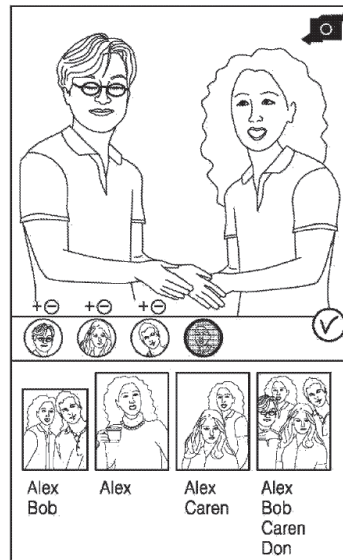
by more than 200 patents issued by the United States Patent and Trademark Office (“USPTO”) to Samsung describing and discussing the use of facial recognition technology, algorithms, and techniques, in general, and in connection with Samsung (hereinafter “Respondents’ Patents”).

76. Samsung’s patents thoroughly describe how its Gallery app applies facial recognition technology. For instance, Patent No.: US 10,666,869 B2: Image Display Apparatus and Image Display Method, issued on May 26, 2020, and Patent No.: US 10,129,481 B2: Image Display Apparatus and Image Display Method, issued on November 13, 2015, confirms Samsung’s use of facial recognition technology and their application of facial processing and recognition technology to every image captured and saved to Samsung’s database:

Referring to FIG. 2 again, in operation S130, the subject included in the captured image may be recognized through face recognition. Whenever the image is captured, the control unit 150 may performed the face recognition on the captured image. The control unit 150 may recognize the subject included in the captured image by comparing a face of the subject included in the captured image with a database. For example, the control unit 150 may recognize the subject included in the captured image within persons included in a contact list. The control unit 150 may separately perform the face recognition on each captured image. The subject may not be included in the captured image, only one subject may be included in the captured image, or two or more subjects may be included in the captured image. Therefore, the number of the subjects recognized from one image through the face recognition may be an integer equal to or greater than 0. In addition, subjects included in different images may be the same person or may be different persons. Therefore, the subject recognized from one image may be identical to or different from the subject recognized from another image. In operation S140, at least one of a tag corresponding to the recognized subject and a share button may be displayed on the camera preview screen. The display unit 120 may display the tag corresponding to the subject recognized from the captured image on the camera preview screen. The tag corresponding to the recognized subject may include a name, a nickname, or a photo of the recognized subject. In addition, the tag may include a symbol, a mark, a word, a phrase, an image, a logo, initials, a user interface, or an icon associated with the recognized subject. The control unit 150 may derive a set of non-overlapped subjects among the entire subjects recognized from the entire captured images. The display unit 120 may display tags corresponding to the subjects included in the derived set in a row. The display unit 120 may display the tags, which are arranged in a row, alongside the photo reel. In addition, the display unit 120 may display the share button on the camera preview screen. The display unit 120 may display the share button alongside the photo

reel. For example, as illustrated in FIG. 4, the display unit 120 may display icons corresponding to the recognized subjects as the tags. According to the embodiment of the present disclosure illustrated in FIG. 4, the control unit 150 may recognize "Alex" and "Bob" from one captured image through face recognition. The display unit 120 may display an icon corresponding to "Alex" and an icon corresponding to "Bob", respectively, as a tag corresponding to "Alex" and a tag corresponding to "Bob". The display unit 120 may display the tags and the share button arranged in a row alongside the photo reel. A subject corresponding to a tag displayed at the leftmost position in FIG. 4 may be "Bob". A subject corresponding to a tag displayed at the second leftmost position in FIG. 4 may be "Alex". As another example, as illustrated in FIG. 6, the display unit 120 may display icons corresponding to the recognized subjects as the tags. According to the embodiment of the present disclosure illustrated in FIG. 5, According to the embodiment illustrated in FIG. 5, the control unit 150 may recognize "Alex" and "Don" from an image corresponding to a thumbnail displayed at the leftmost position. Also, the control unit 150 may recognize "Alex", "Bob", "Caren", and "Don" from an image corresponding to a thumbnail displayed at the fourth leftmost position. In addition, the control unit 150 may recognize "Alex" and "Caren" from an image corresponding to a thumbnail displayed at the fifth leftmost position. The control unit 150 may derive a set including "Alex", "Bob", "Caren", and "Don" as a set of non-overlapped subjects among the entire recognized subjects. The display unit 120 may display tags corresponding to the subjects included in the set in a row.

77. Moreover, as depicted in Figure 4 and Figure 5 below, Samsung's Gallery App operates exactly as explained in Patent Nos. US 10,666,869 and US 10,129,481.

Figure 4⁴⁰**Figure 5⁴¹**

78. Patent No.: US 11,222,196 B2: Simultaneous Recognition of Facial Attributes and Identity in Organizing Photo Albums (Jan. 11, 2022), describes how Samsung applies facial processing technology to recognize facial landmark features to identify and organize photo and video albums based on modifying an efficient convolutional neural network (CNN) which extracts facial representations suitable for face identification and attribute (age, gender, ethnicity, emotion, etc.) recognition tasks.

FIGS. 5A, 5B, and 5C are views of partial implementation of the technique in a mobile application according to various embodiments of the disclosure.

The application may operate in offline mode and does not require Internet connections. *This application sequentially processes all photos from the gallery in a background thread. The demography pane provides stacked histograms (see FIG. 5A) of facial attributes of family members and friends who are present in at least 3 photos from the gallery. Tapping on each black or grey bar within the horizontal stacked histogram in FIG. 5A causes the list of all photos of a particular individual to be displayed (see FIG. 5B).* It is important to emphasize at this point that entire photos rather than just faces extracted therefrom are preferably presented in the display form of the application, so that photos with

⁴⁰ See MemoryWeb, LLC Complaint filed against SEC on April 26, 2021, at pp. 19-22; https://www.docketbird.com/court-documents/MemoryWeb-LLC-v-Samsung-Electronics-Co-Ltd-et-al/COMPLAINT-Filing-fee-402-receipt-number-0542-14738359-No-Summons-requested-at-this-time-filed-by-MemoryWeb-LLC/txwd-6:2021-cv-00411-00001?user_id=guest

⁴¹ See Patent No. US 10,666,869 B2: Image Display Apparatus and Image Display Method (May 26, 2020),

several persons can be exposed in said form. If there are plural individuals with an identical gender and age range, then a spinner can be provided on top of the display form, and said spinner is usable to select a particular person by an associated sequential number (see FIG. 3).

Operation of user device 600 is now described. A *gallery* of the user's video files is inputted to frame selector 611 that is configured to extract high-quality frames. Face detector 612 is configured to detect bounding boxes of *facial* regions in the selected video frames. CNN-based identity feature extractor 613 and CNN-based face attribute recognizer 614 are configured to perform inferences in the CNN according to the disclosure (see FIG. 1) in order to simultaneously extract face identity features and at least some of such *facial* attributes as age, gender, ethnicity, and emotions (see FIG. 2). YoB predictor 615 is configured to compute years of birth associated with the extracted faces given modification dates of respective video files and predicted ages. Frame clusterer 616 is configured to unite identical faces found in different frames of the same video clip.

Now the part of user device 600 that is responsible for processing photos from the *gallery* is described. All the photos are inputted to face detector 621. Face detector 621 is configured to detect a *facial* region(s) in a captured image and resize the *facial* region(s). CNN-based identity feature extractor 622 and CNN-based face attribute recognizer 623 are configured to perform inferences in the CNN according to the disclosure (see FIG. 1). YoB predictor 624 is configured to estimate years of birth associated with the extracted faces.

Next, the rest part of user device 600 that is responsible for demography analysis is described. Face clusterer 630 is configured to group *facial* identity features obtained at the outputs of frame clusterer 616 and CNN-based identity feature extractor 622. Face clusterer 630 may be configured to additionally use the extracted *facial* attributes in order to prevent individuals with significantly different predictions of year of birth from being united by using the outputs of YoB predictors 615, 624. Cluster filter 640 is configured to filter out inappropriate clusters, e.g. clusters with little number of elements or clusters with photos/videos made in one day. The resultant groups of persons and their attributes may be sent to display 650 for providing the user with desired visual output (see FIG. 5, for example). On the other hand, said groups and associated attributes may be provided to a special processing unit (not shown) of user device 600 that is configured to take a decision on allowability of further interactions between the user and the user device based on results of the recognitions with respect to the user, and, based on the decision, either grant the user with the permission for the interactions or deny them.⁴²

⁴² Patent No.: US 11,222,196 B2: Simultaneous Recognition of Facial Attributes and Identity in Organizing Photo Albums (Jan. 11, 2022)

D. Samsung's BIPA Violations Expose Claimant to Threats of Serious Harm.

79. Samsung does not delete the biometrics it collects, which are located on numerous devices in this State. A Samsung Device user's biometrics may be stored on one or more Samsung Devices in use, as well as on discarded Samsung Devices.

80. Furthermore, non-users' biometrics that Samsung collects may be stored on one or more Samsung Devices as well as on discarded Samsung Devices. For example, an Illinois resident's biometrics may be stored on his or her own Samsung Device(s) and/or on the Samsung Devices of his or her family members, relatives, friends, coworkers, and anyone else who photographed him or her using a Samsung Device or stored a photograph of him or her on a Samsung Device. Information stored in a central location, such as a server, presents a single breach threat. A sophisticated entity may take measures to securely and centrally store information, guarding against the threat of a data breach.

81. By contrast, as the result of the fact that the biometrics Samsung collects are stored on numerous devices, Claimant faces the imminent threat of disclosure of their biometrics as a result of a data breach on any one of the Samsung Devices.

82. Samsung has nearly a 30% market share of the smartphone market in the United States,⁴³ and a 17.6% market share of the tablet market.⁴⁴ 85% of adult Americans use smartphones, and 53% use tablets.⁴⁵

⁴³ Chance Miller, *Canalys: Apple Shipped 14.6M iPhones in North America During Q1, Securing 40% Marketshare*, 9to5Mac (May 9, 2019 3:23 PM), <https://9to5mac.com/2019/05/09/iphone-north-america-marketshare/>

⁴⁴ Tablet Vendor Market Share United States of America (June 2021), available at <https://gs.statcounter.com/vendor-market-share/tablet/united-states-of-america>.

⁴⁵ *Mobile Fact Sheet*, Pew Research Center (Apr. 7, 2021), available at <https://www.pewresearch.org/internet/fact-sheet/mobile/>.

83. Many of the Samsung Devices used in this State have collected the biometrics of multiple individuals other than the Samsung Device user. Consequently, numerous Illinois residents have their biometrics stored on one or more Samsung Devices outside their control.

84. The durability of the memory in Samsung Devices creates a near-permanent risk of a data breach of biometric identifiers and information for both device users as well as nonusers whose biometrics have been collected. Samsung Devices utilize solid state memory, which can withstand drops, extreme temperatures, and magnetic fields.⁴⁶

85. Unless corrupted, this solid state memory and the information it contains can last in perpetuity. Thus, the biometrics on Samsung Devices will likely outlast the device battery, the functionality of the device screen, and the natural life of the device user.

86. Biometrics may persist on discarded Samsung Devices, which could be extracted by malicious actors using methods of removal that may or may not currently exist.⁴⁷ The risk of illicit harvesting of biometrics from discarded Samsung Devices therefore extends far into the future.

IV. CLAIMANT'S EXPERIENCE

87. Claimant owns a Samsung Device and has stored photos in the Gallery App.

88. Claimant was never notified of and has never consented to Respondents' use, collection, and storage of Claimant's biometric data.

⁴⁶ Roderick Bauer, *SSD 101: How Reliable are SSDs?*, BackBlaze (Feb. 21, 2019), <https://www.backblaze.com/blog/how-reliable-are-ssds/>.

⁴⁷ See, e.g., Josh Frantz, *Buy One Device, Get Data Free: Private Information Remains on Donated Tech*, Rapid7 Blog (Mar. 19, 2019), <https://www.rapid7.com/blog/post/2019/03/19/buy-one-device-get-data-free-privateinformation-remains-on-donated-devices>; Federal Trade Commission, *How to Protect Your Phone and the Data On It*, <https://www.consumer.ftc.gov/articles/how-protect-your-phone-and-data-it>

89. Claimant did not request or give permission – written or otherwise – to Respondents to collect or store biometric identifiers, nor did Claimant receive or sign a written release allowing Respondents to collect or store biometric identifiers.

90. Respondents never even informed Claimant by written notice or otherwise that Claimant could prevent Respondents from collecting, storing, or using biometric identifiers.

91. Likewise, Respondents never provided Claimant with an opportunity to prohibit or prevent the collection, storage, use, or sharing of Claimant’s face geometry or associated biometric information.

92. Respondents never advised Claimant in writing, or otherwise, of any policy to destroy the biometric identifiers that Respondents collected and stored of Claimant’s face.

93. Nevertheless, when Claimant uploaded photos, Respondents automatically detected and located Claimant’s face, analyzed the geometric data relating to the unique contours of Claimant’s face and the distances between Claimant’s eyes, nose, and ears, and used that data to extract and collect Claimant’s scan of face geometry and related data, such as gender, age, race, and location.

94. As a result of Respondents’ unauthorized collection and use of Claimant’s biometric identifiers, Claimant was deprived of their control over that valuable information.

COUNT I
Violation of the Illinois Biometric Information Privacy Act
(Violation of 740 ILCS 14/15(a))

95. Claimant incorporates the foregoing allegations as if fully set forth herein.

96. Section 15(a) of BIPA requires that any

private entity in possession of biometric identifiers . . . must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers . . . when the initial purpose for collecting or

obtaining such identifiers . . . has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.

740 ILCS 14/15(a).

97. Respondents does not publicly provide a retention schedule or guidelines for permanently destroying Claimant's biometric identifiers as specified by BIPA. *See* 740 ILCS 14/15(a).

98. Accordingly, Claimant seeks: (i) injunctive and equitable relief as is necessary to protect the interests of Claimant by requiring Respondents to establish and make publicly available a policy for the permanent destruction of biometric identifiers compliant with 740 ILCS 14/15(a); and (ii) statutory damages of \$5,000 for this intentional violation of BIPA pursuant to 740 ILCS 14/20(2), or at minimum, \$1,000 for this negligent violation of BIPA pursuant to 740 ILCS 14/20(1).

COUNT II

Violation of the Illinois Biometric Information Privacy Act (Violation of 740 ILCS 14/15(b))

99. Claimant incorporates the foregoing allegations as if fully set forth herein.

100. BIPA makes it unlawful for any private entity to, among other things,

(b) collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:

(1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;

(2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

(3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

....

(d) No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:

(1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure[.]

740CS 14/15(b) and (d).

101. Respondents is a Delaware corporation and thus qualifies as a private entity" under BIPA. *See* 740 ILCS 14/10.

102. Respondents violated section (b) in three ways by: (1) generating, (2) collecting, and (3) storing Claimant's biometric data and information without consent.

103. As explained in detail in Section I above, Claimant's faceprints or face geometry are "biometric identifiers" pursuant to 740 ILCS 14/10.

104. Respondents systematically and automatically collected, used, and stored Claimant's biometric identifiers without first obtaining the specific written release required by 740 ILCS 14/15(b)(3) and (d).

105. As explained above, Respondents did not properly inform Claimant in writing that Claimant's biometric identifiers were being collected and stored, nor did it inform Claimant in writing of the specific purpose and length of term for which these biometric identifiers were being collected, stored, and used, as required by 740 ILCS 14/15(b)(1)–(2).

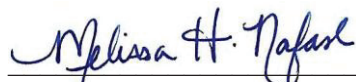
106. By collecting, storing, using, and sharing Claimant's biometric identifiers as described herein, Respondents violated Claimant's right to privacy of these biometric identifiers, as set forth in BIPA, 740 ILCS 14/1, *et seq.*

107. Claimant seeks: (i) injunctive and equitable relief as is necessary to protect the interests of Claimant by requiring Respondents to comply with BIPA's requirements for the collection, storage, and use of biometric identifiers; and (ii) statutory damages of \$5,000 for this intentional violation of 740 ILCS 14/15(b) of BIPA pursuant to 740 ILCS 14/20(2), or at minimum, \$1,000 for this negligent violation of BIPA pursuant to 740 ILCS 14/20(1).

PRAYER FOR RELIEF

WHEREFORE, Claimant respectfully requests that the Arbitrator enter an Order:

1. Declaring that Respondents' actions, as set forth above, violate BIPA, 740 ILCS 14/1, *et seq.*
2. Awarding statutory damages of at least \$15,000;
3. Awarding injunctive relief and ordering that Samsung immediately destroy the faceprints, face scans, and facial geometry of the Claimant;
4. Awarding other equitable relief as is necessary to protect the interests of Claimant, including, inter alia, an order requiring Respondents to collect, store, use, and share biometric identifiers or biometric information in compliance with BIPA;
5. Awarding such other and further relief as equity and justice may require.



LABATON SUCHAROW LLP

Melissa H. Nafash

Jonathan Gardner

Shannon K. Tully

140 Broadway

New York, NY 10005

Tel: (212) 907-0700

Fax: (212) 818-0477

mnafash@labaton.com

jgardner@labaton.com

stully@labaton.com

Counsel for Claimant